UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
Civil Action No. 3:24-cv-654

WILLIAM GASKINS, *on behalf of himself and all others similarly situated*, Plaintiff, v. EVOLVE BANK & TRUST, Defendant.	)	**CLASS ACTION COMPLAINT (JURY TRIAL DEMANDED)**

Plaintiff William Gaskins ("Plaintiff"), on behalf of himself and all other similarly situated, brings this Class Action Complaint against Defendant Evolve Bank & Trust ("Defendant" or "Evolve") and alleges the following:

I. INTRODUCTION.

1. As further set forth and alleged against the individual Defendants, this class action arises out of the data breach ("Data Breach") involving Defendant.[1]

2. Defendant is a bank offering financial services directly to individuals and to third-party companies that provide other financial services directly to individuals, such as Shopify, EarnIn, Branch, Bond, and Mastercard.

3. Plaintiff's dealings with Defendant occurred through Plaintiff's "Dave Debit Card" designed by Dave Operating LLC (d/b/a "Dave Inc."), a digital banking service provider. Defendant is the issuer of the Dave Debit Card and provides the related banking services through a license with Mastercard.

[1] *See generally* Evolve, *News: Cybersecurity Incident*, Jun. 26, 2024 (the "Notice," attached as Exhibit A).

4. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") that it collected and maintained as part of its regular business practices, including but not limited to names, Social Security numbers, dates of birth, account information, and other personal information.

5. Upon information and belief, Dave Inc. contracts all financial services to Defendant, including the collection, maintenance, storage, and security of all PII.

6. Upon information and belief, in order to use Defendant's financial services, former and current customers, including Plaintiff, are required to entrust Defendant with sensitive, non-public PII without which Defendant could not perform their regular business activities.

7. By obtaining, collecting, using, and deriving a benefit from the PII of consumers, including Plaintiff and Class Members, Defendant assumed legal and equitable duties to protect and safeguard that information from unauthorized access and intrusion.

The Data Breach.

8. On June 26, 2024, Defendant announced it was "currently investigating a cybersecurity incident involving a known cybercriminal organization that appears to have illegally obtained and released on the dark web the data and personal information of some Evolve retail bank customers and financial technology partners' customers." (Ex. A).

9. According to Defendant's Notice of Cybersecurity Incident online posting (the "Notice"), the compromised PII included some of the most private information individuals can possess, including but not limited to full names, Social Security numbers, dates of birth, and bank account information. (*Id.*).

10. Defendant failed to adequately protect the PII of its customers, including Plaintiff and Class Members.

11. Defendant failed to even encrypt or redact this highly sensitive information, thus the unencrypted, unredacted PII was compromised and published on the dark web as a direct and proximate result of Defendant's negligent acts and omissions and utter failure to protect sensitive data.

12. Cybercriminals targeted and obtained the PII of Plaintiff and Class Members because of the inherent value in exploiting and stealing their identities. The present and continuing risk to victims of the Data Breach, including Plaintiff and Class Members, will remain for the rest of their respective lifetimes.

13. Defendant failed to provide Plaintiff and Class Members with timely and adequate notice of the Data Breach, including but not limited to information about how the Data Breach occurred; when it occurred; and when Plaintiff's and Class Members's information was released onto the dark web.

14. Until Defendant issued the Notice, Plaintiff and Class Members were entirely unaware that their most sensitive PII had been compromised; and that they were, and continue to be, at significant risk of identity theft and numerous other personal, social, and financial harm.

15. Plaintiff provided his PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his PII. If Plaintiff had known Defendant would not adequately protect his PII, he would never have entrusted Defendant with or allowed Defendant to maintain his sensitive PII.

Relief Sought by Plaintiff and the Class.

16. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to adequately protect the PII of Plaintiff and Class Members; to warn Plaintiff and Class Members of Defendant's inadequate information security practices; and

to effectively secure the technology containing the PII using reasonable and effective security procedures, free of vulnerabilities and incidents. Defendant's conduct, at a minimum, constitutes negligence and violates federal and state statutes.

17. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of its customers, including Plaintiff and Class Members, was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

18. As a result of Defendant's conduct, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered injuries, including, *inter alia*:

a. Invasion of privacy;

b. Lost or diminished value of their PII;

c. Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

d. Loss of benefit of the bargain; and

e. The continued and increased risk to their PII, which remains both unencrypted and available for unauthorized third parties to access and abuse; and stored in Defendant's possession, subject to further unauthorized disclosures until Defendant affirmatively undertakes appropriate and adequate measures to protect the PII as required.

19. Plaintiff and Class Members seek to remedy these injuries and prevent any future compromise of the PII entrusted to Defendant on behalf of himself and all others similarly

situated, whose personal data was compromised and stolen as a result of the Data Breach and thus remain at risk due to Defendant's inadequate data security practices.

20. Moreover, Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. THE PARTIES.

21. Plaintiff is a citizen and resident of North Carolina and is neither an infant, incompetent, nor in the military service of the United States of America.

22. Defendant Evolve Bank & Trust is a bank organized and existing under the laws of Arkansas, with its principal place of business located in Memphis, Tennessee. Evolve is registered to do business in North Carolina, and its registered office is located at 2626 Glenwood Avenue, Suite 550, in Raleigh, North Carolina.

III. JURISDICTION & VENUE.

23. The foregoing allegations are incorporated by reference and realleged herein.

24. Plaintiff is a natural person and resident of North Carolina; a substantial portion of the violations giving rise to this action occurred in North Carolina; and Defendant is registered to do business in North Carolina and conducts considerable business within North Carolina.

25. This Court has subject matter jurisdiction in this matter under 28 U.S.C. § 1332(d), because this is a class action with an amount in controversy exceeding $5,000,000.00 exclusive of interest and costs; there are more than 100 members in the Proposed Class; and more than one member of the Proposed Class, including Plaintiff, are citizens of a different state than Defendant.

26. This Court has personal jurisdiction in this matter because a substantial portion of the violations giving rise to this action occurred in North Carolina; and Defendant is registered to do business in North Carolina and conducts considerable business within North Carolina.

27. Venue is proper under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred within this District and Defendant does business in this District.

IV. FACTUAL ALLEGATIONS.

28. The foregoing allegations are incorporated by reference and realleged herein.

A. Defendant's Business.

29. As stated *supra*, Defendant is a bank offering financial services to its customers, including but not limited to checking accounts, savings accounts, debit cards, personal loans, and financial management services, including through the Dave Debit Card.[2]

30. Plaintiff and Class Members are current and former Evolve customers who used Evolve for banking or other financial services.

31. To open a financial account, apply for financing, or otherwise obtain financial services from Evolve, Plaintiff and Class Members were required to provide multiple categories of sensitive and confidential PII, including but not limited to their names, dates of birth, Social Security numbers, and other financial account information.

32. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of receiving financial services would be kept safe and confidential; that the

[2] *See* Evolve, *Homepage: Personal Banking*, https://www.getevolved.com/personal/ (last accessed Jul. 11, 2024); *see also* Dave Inc., *Homepage: Spending Account*, https://dave.com/spending-account (last accessed Jul. 11, 2024).

privacy of that information would be maintained; and that Defendant would delete any sensitive information it was no longer required to maintain.

33. Indeed, Defendant's Privacy Policy provides that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law…includ[ing] computer safeguards and secured files and buildings."[3]

34. Accordingly, Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII and have taken reasonable steps to maintain the confidentiality of their PII, and they relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

36. Defendant has a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

37. Defendant has a legal duty to keep consumer's PII safe and confidential.

38. Defendant had obligations created by FTC Act, the Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

[3] *See* Evolve, *Consumer Privacy Policy*, Dec. 2022, https://www.getevolved.com/wp-content/uploads/2023/03 /Evolve-Consumer-Privacy-Policy-Notice-12-22-Final.pdf (last accessed Jul. 11, 2024).

39. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. The Data Breach.

41. Defendant failed to utilize reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed. The failure caused the exposure of Plaintiff and Class Members' PII.

42. As a result of Defendant's failure, the cybercriminals accessed and acquired files in Defendant's computer systems containing the unencrypted PII of Plaintiff and Class Members, including, *inter alia*, their names, Social Security numbers, dates of birth, and financial account information. Plaintiff and Class Members' PII was accessed and stolen in the Data Breach.

43. Defendant has admitted that Plaintiff and Class Members' PII has been released onto the dark web. Plaintiff further believes that his PII (and that of Class Members) was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

1. *Defendant Knew or Should Have Known of the Risk of a Data Breach.*

44. As a banking and financial company, Defendant knew or should have known of the substantial risk of a data breach and that its data security obligations to its customers, including Plaintiff and the Class, were particularly important preceding the date of the breach.

45. As custodian of its customers' PII, Defendant knew or should have known the importance of safeguarding the information entrusted to it by its customers, including Plaintiff and the Class, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on victims, including Plaintiff and the Class, as a result.

46. Moreover, with adequate preparedness, data breaches like the one in this case are preventable. As explained by the Federal Bureau of Investigation ("FBI"), "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

47. To prevent and detect cyber-attacks and subsequent exposure of valuable information, Defendant could and should have implemented any variety of reasonable, accessible protective measures[5] for the sensitive PII Defendant knew it was storing from its current and former customers.

---

[4] *See* FBI, *How to Protect Your Networks from Ransomware*, p. 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed July 11, 2024).

[5] *See e.g., Id*., pp. 3-4; U.S. Dept. of Homeland Security – Cybersecurity & Infrastructure Division, *Protecting Against Ransomware*, Apr. 11, 2019, https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed July 11, 2024); and Microsoft, *Human-Operated Ransomware Attacks: A Preventable Disaster*, Mar 5, 2020, https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed July 11, 2024).

48. The occurrence of the Data Breach indicates that Defendant failed to implement adequate protective measures to prevent cyber-attacks, resulting in the Data Breach and the exposure of the PII of thousands of customers, including Plaintiff and Class Members.

2. *Defendant Knew or Should Have Known the Value of the PII in Their Possession.*

49. Defendant knew or should have known that the specific type and significant volume of data on stored in its systems included thousands of individuals' unencrypted, detailed PII; thus, the number of individuals who would be harmed by the exposure of the data would be remarkable.

50. The injuries suffered by Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for Plaintiff and Class Members' PII.

51. The ramifications of Defendant's failure are long-lasting and severe—once PII is stolen (particularly identifiers like Social Security numbers), fraudulent use of that information and damage to victims may continue for years.

52. The Federal Trade Commission ("FTC") defines *identity theft* as "a fraud committed or attempted using the identifying information of another person without authority;" and *identifying information*—the PII—as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," such as "[n]ame, Social Security number, [or] date of birth." 17 C.F.R. § 248.201 (2013).

53. The PII of individuals remains of high value to criminals, as evidenced by the prices paid for PII through the dark web, with online banking login information fetching an average of $100.00 to $150.00. [6]

[6] *See* Ryan Smith, *Revealed – How Much is Personal Information Worth on the Dark Web?*, Insurance Business America – Online, May 1, 2023 (last visited July 11, 2024).

54. Specifically, Social Security numbers are among the most dangerous PII to have compromised because criminals put them to many fraudulent uses. The Social Security Administration stresses that the theft of a person's Social Security number, as experienced by Plaintiff and Class Members (*see* Ex. A), can lead to identity theft and extensive financial fraud because it can be used to obtain other personal information and conduct business in the victim's name, including opening other banking, credit, or utility accounts; receiving medical treatment; stealing the victim's tax refund; and even using the victim's identity if they are arrested.[7]

55. Moreover, the process to change or cancel a stolen Social Security number is often long and arduous, requiring significant amounts of paperwork and evidence of actual misuse.[8]

56. Even then, a new Social Security number may not be effective because the "credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

57. Based on the foregoing, the information compromised in the Data Breach especially harmful because it is uniquely difficult, if not impossible, to change. As a result, Plaintiff and Class Members now face years of stress and expense associated with the constant fear over their financial and personal records, monitoring, and loss of rights; and they will continue to incur damages in addition to any fraudulent use of their PII.

---

[7] *See* Social Security Administration, *Protect Yourself from Identity Thieves*, Apr. 18, 2024, https://blog.ssa.gov/protect-yourself-from-identity-thieves/ (last accessed July 11, 2024).

[8] *See* Social Security Administration, *Identity Theft and Your Social Security Number*, June 2021, pp. 5-6, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 11, 2024) (only after "you've done all you can to fix the problems resulting from misuse" and demonstrated that someone else is actively using your number, the SSA "may assign you a new number;" but the SSA will not issue a new number if, for example, "your Social Security card is lost or stolen, but there's no evidence that someone is using your number.").

[9] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed July 11, 2024).

3. *The Notice.*

58. Despite discovering the Data Breach in May 2024 (by their own admission), Defendant waited until June 26, 2024 to provide any notice to its customers. Plaintiff received notice June 28 via an email from Dave Inc. informing him of the Data Breach, but did not receive any notice from Defendant until July 13.

59. On June 26, Defendant issued a "Notice of Cybersecurity Incident." Defendant published the Notice on its website[10] and sent the Notice to victims of the Data Breach, including Plaintiff and the Class, informing them as follows:

> **What Happened[:]** Evolve is currently investigating a cybersecurity incident involving a known cybercriminal organization that appears to have illegally obtained and released on the dark web the data and personal information of some Evolve retail bank customers and financial technology partners' customers (end users). We take this matter extremely seriously and are working diligently to address the situation. Evolve has engaged the appropriate law enforcement authorities to aid in our investigation and response efforts. Based on what our investigation has found and what we know at this time, we are confident this incident has been contained and there is no ongoing threat.
>
> **What Information Was Involved[:]** It appears these bad actors have released illegally obtained data, including Personal Identification Information (PII), on the dark web. The data varies by individual but may include your name, Social Security Number, date of birth, account information, and/or other personal information.
>
> **What We Are Doing[:]** We are beginning the long process of communicating with customers who have been affected by this incident. If you are impacted, you will receive an email from notifications@getevolved.com with detail instructions on how to enroll in complimentary credit monitoring with identity theft detection services.
>
> **What You Can Do[:]** We encourage customers to remain vigilant by monitoring account activity and credit reports. You can set up free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. You can also request and review your

[10] *See* (Ex. A).

> free credit report at any time via Freecreditreport.com. If you suspect any fraud or suspicious activity please contact us immediately.
>
> If you suspect that you're the victim of identity theft or fraud, you have the right to file a report with the Federal Trade Commission (FTC) or law enforcement authorities.

(Ex. A).

60. Notably, the Notice entirely omitted several critical facts, including: the date Defendant discovered the Data Breach; the details of the Data Breach's root cause; the reasons for the Defendant's delayed discovery of the Data Breach and subsequent notification to affected consumers, including Plaintiff and Class Members; the vulnerabilities exploited; and the remedial measures undertaken by Defendant to ensure such a breach does not occur again.

61. To date, these critical facts have not been explained or clarified to affected consumers, including Plaintiff and Class Members, all of whom still have a vested interest in ensuring that their PII is protected.

62. Moreover, the Notice entirely fails to provide any compensation for the unauthorized disclosure of Plaintiff and Class Members' PII, including the failure to offer identity or credit monitoring services despite the fact that victims of data breaches and other unauthorized disclosures commonly endure years of ongoing identity theft and financial fraud. Instead, Defendant merely suggested that victims, including Plaintiff and the Class, "remain vigilant by monitoring account activity and credit reports" by signing up for "free fraud alerts from nationwide credit bureaus" or reviewing a "free credit report at any time via freecreditreport.com." (Ex. A).

63. As a result, Plaintiff and Class Members are forced to pay out of pocket for necessary identity monitoring services in order to protect themselves from the consequences of Defendant's acts and omissions.

64. Accordingly, the Notice is truly no real "notification" at all, as it fails to inform the Data Breach victims, including Plaintiff and the Class, of the critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

C. Defendant Failed to Comply with the Applicable Law and Industry Standard.

1. *Defendant Failed to Comply with FTC Guidelines.*

65. The FTC has promulgated numerous guides for businesses highlighting the necessity of reasonable data security practices, specifically including cyber-security guidelines for businesses (the "Guidelines").[11]

66. The Guidelines note that businesses who store customers' PII should protect it adequately, including encrypting information and networks; auditing and addressing their vulnerabilities; and implementing policies to correct security problems, or else properly dispose of all PII no longer needed.

67. The Guidelines also recommend an intrusion detection system to expose a breach as soon as it occurs; monitor for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in case of a breach.[12]

[11] *See* FTC, *Protecting Personal Information: A Guide for Business*, 2016, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting- personal-information.pdf (last visited July 11, 2024).
[12] *Id.*

68. The FTC has brought enforcement actions against businesses for failing to adequately protect customer data, treating the failure to employ reasonable and appropriate measures (as demonstrated in the Guidelines) to protect against unauthorized access to confidential information as an unfair act or practice prohibited by the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F.Supp.3d 374, 408 (E.D.Va. 2020).

69. The FTC Act prohibits "unfair…practices in or affecting commerce," including, *inter alia*, the failure to use reasonable measures to protect PII, as interpreted and enforced by the FTC. 15 U.S.C. § 45.

70. The FTC publications and orders, described *supra*, also form part of the basis for Defendant's duty to its customers, including Plaintiff and Class Members, in this case. Accordingly, per the prevailing interpretation of the meaning and effect of the FTC Guidelines and the FTCA, 15 U.S.C. § 45, Defendant breached its duty to its customers by failing to properly implement basic data security practices; and such failure constitutes an unfair act or practice under the FTCA, 15 U.S.C. § 45.

71. Upon information and belief, at all relevant times, Defendant was fully aware of its obligation to protect the PII of its customers, including Plaintiff and the Class, pursuant to the FTC Guidelines and the FTCA; and of the significant repercussions likely to result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained, used, and stored, and the foreseeable, immense damages that would result for Plaintiff and the Class.

2. *Defendant Failed to Comply with Industry Standards*.

72. As described *supra*, experts studying cybersecurity routinely identify financial entities like Defendant as being particularly vulnerable because of the amount and value of the PII they collect and maintain; and several authorities have identified and published industry standards and best practices for financial entities in possession of consumers' PII, like Defendant, for protecting such sensitive data, which Defendant plainly failed to implement.

73. Defendant's failure to comply with the existing and applicable industry standards opened the door to the threat of a cyber-attack and ultimately caused the Data Breach.

D. Plaintiff's Factual Allegations.

74. Plaintiff has a debit card account with Dave Inc., which partners with Defendant to provide banking-related services for consumers. In order to receive banking products and services through that partnership, Plaintiff was required to provide Defendant with multiple categories of PII, including but not limited to his full name, Social Security number, date of birth, email address, and physical address.

75. Plaintiff entrusted his PII to Defendant with the reasonable expectation and understanding that Defendant would—at a minimum—implement precautionary measures to protect his PII consistent with the industry standards; and would timely notify him of any cybersecurity incidents involving him or his PII. Plaintiff would not have permitted Defendant to take possession of his PII had he known Defendant would not take reasonable steps to safeguard his PII.

76. Nonetheless, on or about June 28, 2024, Plaintiff received an email from Dave Inc. informing him of a "cybersecurity incident" involving their partner bank, Defendant Evolve. Though Evolve discovered the Data Breach in May, this June 28 email was Plaintiff's first indication that any of his PII could be compromised.

77. As a result of the Data Breach, Plaintiff is now required to mitigate its impact for the rest of his life, including but not limited to either undertaking continuous reviews of his credit reports, financial account statements, and personal records for any indications of actual or attempted identity theft or fraud on his own; or incurring costs for monitoring services.

78. As a result of the Data Breach, Plaintiff suffered actual injury from having his PII compromised, including, *inter alia*: (a) damage to and diminution in the value of his PII—a property interest that Defendant obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

79. As a result of the Data Breach, Plaintiff is extremely concerned about the occurrence and consequences of identity theft and fraud, particularly given the nature of the PII he entrusted to Defendant.

80. As a result of the Data Breach, Plaintiff has suffered and will continue to suffer significant anxiety and stress, compounded by the fact that his PII, including his Social Security number, are in the hands of cybercriminals.

81. As a result of the Data Breach, Plaintiff will be at present, imminent, and continued increased risk of identity theft and fraud for years to come, and he anticipates spending considerable time and money continuously to try to mitigate the direct and incidental harms caused by Defendant's failure to protect his PII.

82. Upon information and belief, Plaintiff's PII remains in Defendant's possession, thus Plaintiff has a strong, continuing interest in ensuring that his PII—as well as all Class Members' PII—is fully protected from any future breaches.

V. CLASS ALLEGATIONS.

83. The foregoing allegations are incorporated by reference and realleged herein.

84. Plaintiff brings this class action on behalf of themselves and on behalf of all others similarly situated, seeking to represent a **Nationwide Class** and the **North Carolina Subclass,** and defined *infra*.

85. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action both individually and as a proposed class action against Defendants on behalf of the **Nationwide Class,** defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach.

86. Moreover, pursuant to Rule 23 of the North Carolina Rules of Civil Procedure, Plaintiff brings this action both individually and on behalf of a **North Carolina Subclass,** defined as follows:

> All individuals residing in North Carolina whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach.

87. Plaintiff reserves all rights to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

88. Expressly excluded from the Class are: (1) any Judge presiding over this action and members of their families; (2) each Defendant and any entity in which each Defendant has a controlling interest, or which have a controlling interest in any Defendant, and Defendants' current or former employees, investors, members, or officers; and (3) all persons who properly execute and file a timely request for exclusion from the Class.

89. ***Numerosity*****:** Members of the Classes are so numerous that their individual joinder is impracticable, if not impossible. While the precise number is unknown at this time, upon information and belief, the proposed Classes are composed of thousands of individuals who were and are being notified by Defendant of the Data Breach. Moreover, Class Members' identities will be easily ascertainable and identifiable from through a review of Defendants' business records.

90. ***Commonality*****:** Questions of law and fact common to the members of the Classes predominate over questions affecting only individual members. Such common questions include but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

d. When Defendant actually learned of the Data Breach, and whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages due to Defendant's wrongful conduct; and

i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

91. ***Typicality*****:** Plaintiffs' claims are typical of the claims of the members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as all other Class Members.

92. ***Adequate Representation*****:** Plaintiff will fairly and adequately protect the interests of the Classes, and he has no interests antagonistic to those of the Classes. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members. Plaintiff has retained counsel experienced in the prosecution of construction defect claims and complex litigation, including home defect claims and class actions.

93. ***Predominance and Superiority*****:** This class action is appropriate for certification because questions of law and fact common to the Class Members predominate over questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy, since individual joinder of all members of the class is impracticable. If individual Class Members are required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system, while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action

presents far fewer management difficulties, while providing unitary adjudication, economies of scale, and comprehensive supervision by a single Court. There is no unusual difficulty in the management of this action as a class action—Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Moreover, adequate notice can be given to Class Members directly using information maintained in Defendant's records

VI. CAUSES OF ACTION.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of the Nationwide Class and the North Carolina Subclass).

94. The foregoing allegations are incorporated by reference and realleged herein.

95. Defendant requires their customers, including Plaintiff and Class Members, to submit sensitive PII in the ordinary course of providing financing services; thus, Plaintiff and Class Members entrusted Defendant with their PII for the purpose of securing financial or other services from Defendant.

96. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

97. As described *supra*, Defendant had a duty to employ reasonable security measures under the FTCA, which prohibits, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. *See* 15 U.S.C. § 45.

98. Defendant's duty of care to use reasonable security measures also arose via the special relationship that existed between Defendant and its banking customers, including Plaintiff and Class Members, when they entrusted Defendant with their confidential PII as a necessary part of receiving financial services.

99. Defendant's duty of care to use reasonable security measures also arose via the well-established banking industry standards regarding the protection of confidential PII.

100. Defendant breached its duties, and thus was negligent in failing to use reasonable measures to protect Class Members' PII. The specific acts and omissions include, *inter alia*:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

101. Moreover, Defendant violated the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail *supra*. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Classes. Defendant's violation of the FTCA constitutes prima facie evidence of negligence.

102. Plaintiff and Class Members are within the class of persons that the applicable law, including the FTCA, was intended to protect.

103. The Data Breach and resulting injury to Plaintiff and the Classes was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

104. Defendant had and has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Classes could and would suffer if the PII were wrongfully disclosed.

105. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

106. Plaintiff and the Classes had no ability to protect their PII that was in, and possibly remains in, Defendant's possession; only Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

107. Defendant had and has a duty to adequately notify Plaintiff and the Classes that their PII within Defendant's possession might have been compromised, how and when it was compromised, and precisely the types of data that were compromised. Such notice was

necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

108. Defendant admitted that the PII of Plaintiff and the Classes were wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach. (*See* Ex. A).

109. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised.

110. There is a close causal connection between Defendant's failure to implement security measures to protect its customers' PII and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

111. The PII of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding the PII by adopting, implementing, and maintaining appropriate security measures.

112. Accordingly, as a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will continue to suffer injury, including but not limited to: (a) invasion of privacy; (b) lost or diminished value of PII; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their PII, which remains stored, unencrypted, in Defendant's possession and is therefore subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

113. As a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and harm, including but not

limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

114. As a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as it fails to undertake appropriate and adequate measures to protect the PII in its possession.

115. Accordingly, Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach; as well as injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class and the North Carolina Subclass).

116. The foregoing allegations are incorporated by reference and realleged herein.

117. As explained *supra*, Plaintiff and Class Members were required to provide their PII to Defendant as a condition of obtaining services from Defendant; and in reasonable reliance upon, *inter alia*, Defendant's promise to protect their PII from unauthorized disclosure and to delete it once it was no longer required to maintain it.

118. Upon information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.[13]

[13] Plaintiff incorporates Defendant's Privacy Policy herein: https://www.getevolved.com/wp-content/uploads/2023/03/Evolve-Consumer-Privacy-Policy-Notice-12-22-Final.pdf (last visited: July 11, 2024).

119. Upon information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff and Class Members' PII would remain protected.

120. Implicit in the agreement between Defendant and its customers, including Plaintiff and the Classes, to provide PII was Defendant's obligation to: (a) use PII for business purposes only; (b) take reasonable steps to safeguard PII; (c) prevent unauthorized disclosures of PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; (f) retain the PII only under conditions that kept such information secure and confidential; and (g) delete or destroy PII after it was no longer necessary to retain it.

121. When Plaintiff and Class Members provided their PII to Defendant as a condition of receiving banking and financial services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to delete or destroy it following the end of the business relationship.[14]

122. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

123. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security and retention practices complied with relevant representations, laws, and regulations and were consistent with industry standards.

[14] *Id.*

124. In providing their PII to Defendant, Plaintiff and Class Members reasonably relied upon Defendant's Privacy Policy, which specifically outlines lawful disclosures of PII, none of which apply in this case.[15]

125. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

126. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to delete their PII once it was no longer necessary.

127. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

128. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

129. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII.

130. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

131. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach; to nominal damages for the breach of implied contract; and to injunctive relief, as defined *supra*.

[15] *Id.*

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
In the Alternative
(On Behalf of the Nationwide Class and the North Carolina Subclass).

132. The foregoing allegations are incorporated by reference and realleged herein.

133. This Cause of Action is pleaded in the alternative to Breach of Implied Contract, *supra*.

134. Plaintiff and Class Members conferred a monetary benefit to Defendant when they provided their PII and payment for Defendant's financial services.

135. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant, and it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of PII to Defendant from Plaintiff and Class Members is an integral part of Defendant's business. Without collecting and maintaining Plaintiff's and Class Members' PII, Defendant would be unable to offer financial services.

136. Defendant was supposed to use some of the monetary benefit provided to it by Plaintiff and Class Members to secure the PII belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

137. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the PII of Plaintiff and Class Members.

138. Defendant gained access to the Plaintiff's and Class Members' PII through inequitable means because Defendant failed to disclose that it used inadequate security measures.

139. Plaintiff and Class Members were unaware of the inadequate security measures and would not have entrusted their PII to Defendant had they known of the inadequate security measures.

140. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

141. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) lost or diminished value of PII; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their PII, which remains stored, unencrypted, in Defendant's possession and is therefore subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

142. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

143. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class and the North Carolina Subclass).

144. The foregoing allegations are incorporated by reference and realleged herein.

145. In providing their PII to Defendant, Plaintiff and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiff and Class Members to safeguard and keep confidential that PII.

146. Defendant accepted the special confidence Plaintiff and Class Members placed in it, as evidenced by its acknowledgement that it had a legal duty to protect Plaintiff and Class Members' PII.

147. In light of the special relationship between Defendant and its customers, including Plaintiff and Class Members, whereby Defendant agreed to be a guardian of their PII, Defendant became a fiduciary and promised to act primarily for the benefit of its customers, including Plaintiff and Class Members, including the safeguarding PII.

148. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customer relationships, in particular, to keep secure the PII of its customers.

149. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing their PII.

150. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard their PII.

151. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of the services they paid for and received.

152. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm and other economic or non-economic loss.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf the Nationwide Class and the North Carolina Subclass).

153. The foregoing allegations are incorporated by reference and realleged herein.

154. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

155. Furthermore, the Court has broad authority to restrain acts, including Defendant's acts and omissions here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

156. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff and Class Members' PII; and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII.

157. Plaintiff alleges that Defendant's data security measures remain inadequate, and as such Plaintiff and the Classes will continue to suffer injury remain at imminent risk that further compromises of their PII will occur in future.

158. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant, *inter alia*:

a. Owes a legal duty to secure its customers' PII, including that of Plaintiff and Class Members, and to timely notify them of a data breach under applicable law; and

b. Continues to breach this legal duty by failing to employ reasonable measures to secure such PII.

159. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and the Classes will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, thus they will be forced to bring multiple lawsuits to rectify the same conduct.

160. The hardship to Plaintiff and the Classes if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class Members will likely suffer substantial identity theft and other damage; while the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal and Defendant has a pre-existing legal obligation to employ such measures.

161. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to consumers whose confidential information would be further compromised, including Plaintiff and the Classes.

VII. PRAYER FOR RELIEF.

WHEREFORE, Claimant respectfully requests that this Court:

a. Certify the Classes defined herein, appoint Plaintiff as Class Representative, and appoint Plaintiff's undersigned counsel as Class Counsel to represent the Classes;

b. Enjoin Defendant from engaging in the wrongful conduct described herein, and from refusing to issue prompt, complete, and accurate notification to Plaintiff and Class Members;

c. Grant injunctive relief requested by Plaintiff;

d. Grant an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. Grant an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

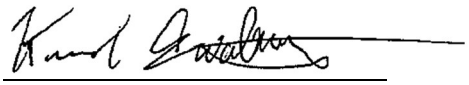
f. Grant an award of pre- and post-judgment interest on all amounts awarded;

g. Allow a trial by jury on all issues so triable; and

h. Grant Plaintiff and the class members such other and further relief as the Court deems just and proper.

Respectfully submitted, this the 15th day of July, 2024.

MAGINNIS HOWARD



KARL S. GWALTNEY
N.C. State Bar No. 45118
EDWARD H. MAGINNIS
N.C. State Bar No. 39317
7706 Six Forks Road, Suite 101
Raleigh, North Carolina 27615
Tel: 919-526-0450
Fax: 919-882-8763
kgwaltney@carolinalaw.com